

The HIPAA Privacy and Transactions Rules

Gail Horlick, MSW, JD

National Breast and Cervical Cancer Early Detection Program

Data Managers' Meeting

Boston, MA

May 30, 2002

Overview

- Current status of legal protection for confidential health care information
- Health Insurance Portability and Accountability Act of 1996 (HIPAA)
 - Privacy rule
 - Potential impact of HIPAA privacy rule on public health
 - Transactions Rule

Legal Protection of Confidential Health Care Information

- No comprehensive federal law
 - Privacy Act
 - Substance abuse laws
 - Video rental laws
 - Inconsistent and conflicting state laws
 - Disease specific statutes
 - Professional practice acts, hospital licensure laws, civil and criminal statutes

HIPAA Administrative Simplification Provisions

- HIPAA Administrative Simplification provisions address privacy and security
- Require the development of:
 - Privacy legislation or regulations
 - Standards for transactions and code sets
 - Standards for security

HIPAA Privacy Requirements

- Congress required to enact federal privacy legislation by 8/99 or Secretary Department of Health and Human Services (DHHS) was to issue regulations
 - Congress did not meet the deadline
- 11/99: Draft privacy regulations published in Federal Register

–over 52,000 comments received

Final HIPAA Privacy Rule

- 12/28/00: Final privacy rule published
- 2/01: Secretary DHHS reopened privacy rule for 30-day comment period
- Over 11,000 comments received
- 3/27/02: Proposed rule modifications published
- 30 day comment period
- Comments will be analyzed and final privacy rule will be published

Privacy Rule Compliance Dates

- 4/14/01: Final privacy rule went into effect
- 4/14/03: Compliance Date
- 4/14/04: Compliance date for small health plans

Scope Of Privacy Rule (1)

- HIPAA limits scope of privacy rule
- Scope is narrower than scope of comprehensive privacy legislation
- Rule applies to Covered Entities (CE):
- Health plans
- Health care clearinghouses
- Health care providers (those who transmit certain health claims information electronically) (§164.104)

Scope Of Privacy Rule (2)

- Many provisions of rule apply indirectly to Business Associates (BA)
- BA hired to perform functions or activities on behalf of CE
- E.g. legal or accounting services, utilization review, claims processing
- CE needs satisfactory assurance, usually a contract or memoranda of understanding, that BA will safeguard information

Scope Of Privacy Rule (3)

- Rule governs the use and disclosure of Protected Health Information (PHI)
- PHI:
- Relates to person's physical or mental health or provision or payment for health care

- Identifies, or could be used to identify person who is subject of information
- Is created or received by CE
- Is transmitted or maintained in any medium (§164.501)

HIPAA Privacy Rule

Protects:

- all individually identifiable health information
- in any form, electronic or non-electronic
- that is held or transmitted by a covered entity or its BA

Individual Rights

Privacy rule gives individuals the right to:

- Inspect and obtain copy of PHI
- Request amendment of information or have statement of disagreement included
- Request restrictions on uses and disclosures
- Have reasonable requests for confidential communication accommodated
- An accounting of disclosures
- File a written complaint (without retaliation)

Relationship Of Privacy Rule To Federal and State Laws (1)

- CE subject to other federal laws and regulations (e.g. Privacy Act of 1974)
- Privacy rule preempts state laws that are contrary to rule (§160.203)
- Limited exceptions such as fraud and abuse

Relationship Of Privacy Rule To Federal and State Laws (2)

- Does not preempt more stringent state privacy laws
- Provides a floor
- Does not preempt laws “for the conduct of public health surveillance, investigation, or intervention...” (§160.203(a)(2)(c))

Potential Implications Of Privacy Rule For Public Health

- Intent of law and rule
- Disclosure to public health authorities
- Responsibilities of covered entities

Intent Of Rule Regarding Public Health

Analysis of comments in preamble to privacy rule refers to mandate in HIPAA:

“Nothing in this part shall be construed to invalidate or limit the authority, power or procedures established under any law providing for the reporting of disease or injury, child abuse, birth or death, public health surveillance, or public health investigation or intervention.”

Use and Disclosure of PHI

- Providers who transmit information electronically are CE under rule
- Rule states CE must obtain written patient consent (§164.506) or authorization (§164.508) for all uses and disclosures of PHI for treatment, payment, and health care operations (TPO) EXCEPT those specifically listed
- Proposed rule modification does NOT require consent for uses and disclosures for TPO

Disclosure to Public Health (1)

- Consent or authorization is NOT required for uses and disclosures:
 - required by law
 - for certain public health activities
- Rule and proposed modification same regarding disclosure to public health

Disclosure To Public Health (2)

Providers may disclose PHI to public health authorities without consent or authorization:

- If reporting is mandated by law (§164.512(a)(1)) **and/or**
- For certain public health activities and purposes (§164.512(b)(1)(i))

Disclosure To Public Health (3)

Provider may disclose PHI for activities and purposes to:

“...a public health authority that is authorized by law to collect or receive such information for the purpose of preventing or controlling disease,...the conduct of public health surveillance, public health investigations, and public health interventions...”
(§164.512(b)(1)(i))

Public Health Authority

Public health authority means:

- an agent or authority of the US, a State, a territory, a political subdivision of a State or territory, or an Indian tribe,
- or a person or entity acting under a grant of authority from or contract with such public agency, including the employees or agents of such public agency, or its contractors or persons or entities to whom it has granted authority,
- that is responsible for public health mandates as part of its official mandate (§164.501)

Implications For Providers

- Providers (CE) can disclose information to public health without consent:
 - If reporting is mandated by law (e.g. registry law mandates reporting) **and/or**
 - To public health authority authorized by law to collect information for prevention or control of disease
- Specific mandate to report not required
- State law may require consent
- E.g. state registry law may require consent

Implications For Public Health

- Only health plans, clearinghouses, and providers transmitting specified claims electronically are CE
- Non CE are not directly bound by privacy rule
- Privacy rule will not impact use and disclosure of PHI by non CE
- State and local laws and policies will apply
- Program may hold PHI
- Program may have other reasons for compliance with privacy rule

Additional Implications For Public Health

- Doctors, nurses, and other providers of direct service in state and local health departments are CE
- CE must comply with privacy rule

Responsibilities of CE (1)

CE must:

- Follow consent and authorization requirements for use and disclosure of PHI
- Make reasonable efforts to limit use or disclosure of PHI to minimum amount necessary to accomplish their purpose

- Exceptions: disclosure for treatment and to individual

Responsibilities of CE (2)

- CE must:
 - Designate a privacy official
 - Develop policies and procedures (including receiving complaints)
 - Provide privacy training to its workforce
 - Develop sanctions for employees who violate entity's policies and/or privacy rule
 - Meet documentation requirements
 - Other
- Requirements flexible and scalable

Issues To Be Addressed

- Providers' concerns
 - Providers may be advised to have written agreement before disclosure to public health
- HIPAA standards may be viewed as best practices for non CE

HIPAA Transactions Rule

- Standard for Electronic Transactions addresses the electronic transmission of administrative and financial data
- Final transactions rule published 8/17/00
 - includes standards for 8 of the 9 specified electronic transactions in HIPAA §1173(a)(2) and code sets to be used
- Final rule for health claims attachment not published yet

Standards for Electronic Transactions (1)

- Enrollment and disenrollment in health plan
- Eligibility for a health plan
- Health care payment and remittance advice
- Health plan premium payments

Standards for Electronic Transactions (2)

- First report of injury
- Health claim status
- Referral certification and authorization
- Health claims or equivalent encounter information

Transactions Rule: Background

- Before rule, approximately 400 different formats for electronic submission of health claims were being used in US
- Lack of standardization led to need for legislation

Transactions Rule: Applicability

Standards apply to:

- Health plans
- Health care clearinghouses
- Providers who transmit information in electronic form in connection with a transaction referred to in §1173(a)(1) of HIPAA

Transactions Rule: Compliance Date (1)

- Final rule published 8/17/00
- Original compliance date: 10/16/02
 - 10/16/03 for small health plans (< \$5 million in receipts)
- Administrative Simplification Compliance Act allows CE to request a 1 year extension to compliance deadline until 10/16/03 by submitting compliance plan to DHHS

Transactions Rule: Compliance Date (2)

- Compliance plan must be submitted by 10/15/02
- Centers for Medicare and Medicaid Services (CMS) has developed HIPAA Model Compliance Plan
- Plan and online help available at:
<http://www.cms.gov/hipaa2/ASCAForm.asp>

Transactions Rule: Compliance Date (3)

- Plan can be submitted electronically
 - CMS will provide electronic confirmation of receipt
- CE can submit own version of extension plan that provides equivalent information
- Plan can be submitted on paper

For More Information: CDC Resources

- CDC Information Council website: <http://www.cdc.gov/cic>–Click on legislation
- National Immunization Program website:
<http://www.cdc.gov/nip/registry>–Click on Privacy, Confidentiality, Security & Legislation

For More Information:**Office of Civil Rights**

Office of Civil Rights website:

<http://www.hhs.gov/ocr/hipaa>

- Guidance document for rule published 7/6/01
- Allows email submission of questions on privacy rule
- Concerns will be addressed in Frequently Asked Questions or other guidance documents

For More Information: DHHS

DHHS Administration Simplification website:

<http://aspe.os.dhhs.gov/admnsimp>

- Provides current HIPAA information
- Allows email submission of questions on transactions rule
- Can download technical specifications for transaction standard (HIPAA Implementation Guide) for free

Contact Information

Gail Horlick, M.S.W., J.D.

Program Analyst

CDC National Immunization Program

1600 Clifton Rd. NE, MS E-62

Atlanta, Ga. 30333

phone: 404-639-8345

fax: 404-639-8171

email: gyh6@cdc.gov

